(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－204338
（P2003－204338A）
(43)公開日　平成15年７月18日(2003.7.18)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/28	３００	Ｈ０４Ｌ　12/28	３００Ｚ　５Ｋ０３３ ３００Ａ

審査請求　有　　請求項の数11　ＯＬ　（全 14 頁）

(21)出願番号　特願2002－2419(P2002－2419)

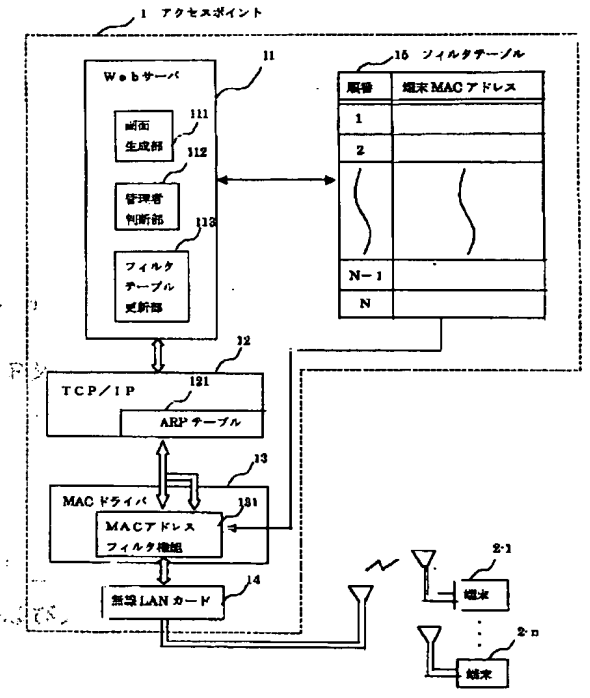
(22)出願日　平成14年１月９日(2002.1.9)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　可知　靖司
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088328
弁理士　金田　暢之　（外２名）

Ｆターム(参考)　5K033 AA08 DA17 DB16 EC03

(54)【発明の名称】　無線ＬＡＮシステム、アクセス制御方法およびプログラム

(57)【要約】
【課題】　認証のための処理が煩雑になることがなく、会議の参加者の中からシステム管理者を設定することのできる無線ＬＡＮシステムを提供する。
【解決手段】　任意の場所に設置可能なアクセスポインタ１と、アクセスポインタ１と無線により相互通信可能に接続される複数の端末２－１～２－ｎとを有する無線ＬＡＮシステムであって、アクセスポインタ１はサーバ１１を有し、サーバ１１は、端末２－１～２－ｎのうちの当該サーバ１１に最初にアクセスしてきた端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、上記システム管理者によって当該サーバ１１へのアクセスが制限される一般ユーザとして扱うように構成されている。



【特許請求の範囲】
【請求項１】　任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線ＬＡＮシステムであって、
前記アクセスポイントはサーバを有し、
前記サーバは、当該サーバにアクセスしてきた前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって当該サーバへのアクセスが制限される一般ユーザとして扱うように構成されている無線ＬＡＮシステム。
【請求項２】　所定の端末が、サーバに最初にアクセスしてきた端末であることを特徴とする請求項１に記載の無線ＬＡＮシステム。
【請求項３】　アクセスポイントはフィルタテーブルをさらに有し、
サーバは、複数の端末のうちの当該サーバにアクセスしてきた端末のＭＡＣアドレスをそのアクセスの順番と対応づけて前記フィルタテーブルに登録し、前記フィルタテーブルに最も早い順番でＭＡＣアドレスが登録された端末をシステム管理者として扱うことを特徴とする請求項２に記載の無線ＬＡＮシステム。
【請求項４】　アクセスポイントは、複数の端末のいずれかからパケットが送出されると、該送出されたパケットについて、その送信元の端末のＭＡＣアドレスを検査するフィルタ処理手段をさらに有し、
サーバは、当該サーバにアクセスしてきた端末のうち、システム管理者によってアクセス許可の設定がなされた端末のＭＡＣアドレスのみを前記フィルタテーブルに登録し、
前記フィルタ処理手段は、前記送出されたパケットの、送信元の端末のＭＡＣアドレスが前記フィルタテーブルに登録されている場合、もしくは、前記送出されたパケットが前記サーバへのアクセスである場合にのみ、そのパケットを通すことを特徴とする請求項３に記載の無線ＬＡＮシステム。
【請求項５】　所定の端末が、サーバにアクセスしてきた端末のうち、自身がシステム管理者となる旨の入力をした端末であることを特徴とする請求項１に記載の無線ＬＡＮシステム。
【請求項６】　任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線ＬＡＮシステムにおいて行われるアクセス制御方法であって、
前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱うアクセス制御方法。
【請求項７】　所定の端末が、サーバに最初にアクセスした端末であることを特徴とする請求項６に記載のアクセス制御方法。
【請求項８】　所定の端末が、サーバにアクセスした端末のうち、自身がシステム管理者となる旨の入力をした端末であることを特徴とする請求項６に記載のアクセス制御方法。
【請求項９】　任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線ＬＡＮシステムにおいて用いられるプログラムであって、
前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱う処理と、
前記所定の端末以外の端末の利用者を、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱う処理とを、前記サーバのコンピュータに実行させるプログラム。
【請求項１０】　所定の端末が、サーバに最初にアクセスした端末であることを特徴とする請求項９に記載のプログラム。
【請求項１１】　所定の端末が、サーバにアクセスした端末のうち、自身がシステム管理者となる旨の入力をした端末であることを特徴とする請求項９に記載のプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データ通信システムに関し、特には無線ＬＡＮ（Local Area Network）システムに関する。さらに、本発明は、そのようなシステムにおいて用いられる、アクセス制御方法およびプログラムに関する。
【０００２】
【従来の技術】最近では、社内のちょっとした会議でも、各参加者が携帯情報端末、例えばノート型ＰＣ（パーソナルコンピュータ）端末を持ち寄って、必要な情報をやり取りするケースが多くなってきた。こういった場合、参加者の間で共有する情報（例えば、参加者に配布される、会議に必要な情報で、ファイル形式でデータ保存される。）は、例えばコンパクトフラッシュ（登録商標）（カードメモリ）などのメディアを用いて各参加者に渡されるが、参加者の人数が多くなると、そういったメディアを用いたファイルの共用は非常に面倒である。そこで、上記のような会議において、参加者の各ＰＣ端末を、ネットワークを介して相互に通信可能に接続することのできるＬＡＮが導入されるようになってきた。
【０００３】ＬＡＮは、基本的に、１つのサーバと、これに相互通信可能に接続される複数の端末（クライアント）とから構成されており、伝送媒体の違いから、有線

ＬＡＮと無線ＬＡＮに分類される。有線ＬＡＮは、通信ケーブルなどを予め敷設しておく必要があり、会議に使用される社内のすべての部屋にそのような敷設を行うことはコストなどの面から難しいことから、上記のような会議への適用は困難である。これに対して、無線ＬＡＮは、通信ケーブルなどの敷設は必要なく、持ち運び可能な一時設置アクセスポイント（Access Point ： ＡＰ）を使用することで、必要なネットワークを任意の場所で構築することができるので、上記のような会議への適用は容易である。

【０００４】無線ＬＡＮの導入に際して問題となるのが、セキュリティである。会議で扱われるデータは、秘匿性の高いものであり、外部に漏れることを避けるためには、無線ＬＡＮに対する第三者からのアクセスを何らかの形で制限する必要がある。このような制限を行うために、通常は、無線ＬＡＮのネットワークＯＳ（オペレーティングシステム）がセキュリティ機能を備えている。

【０００５】セキュリティ機能には、例えば、登録されたユーザが正しいパスワードを提示した場合にのみサーバへのログインを認めるネットワークアクセスの制御や、ファイルへのアクセス権を特定のユーザに限定するファイルへのアクセス制御などの他、ユーザの登録などを管理するユーザ管理やシステム管理などを特別な権限を持つシステム管理者に限定する制御がある。システム管理者は、このセキュリティ機能を用いて、決められたクライアントに対してのみサーバへのアクセスを許可することができ、これにより、第三者による不正なアクセスを制限することができる。

【０００６】また、よりセキュリティを高めるために、ＭＡＣ（Medium Access Control :媒体アクセス制御）アドレスを検査するパケットフィルタ機能により、第三者による不正なアクセスを制限するものがある。ここで、ＭＡＣアドレスは、物理アドレスであって、送信先アドレスおよび送信元アドレスである。図８は、そのようなＭＡＣアドレスを利用したアクセス制限を行う無線ＬＡＮシステムの概略構成図である。

【０００７】図８において、無線ＬＡＮの基地局としてのアクセスポイント（ＡＰ）１０１と、ＡＰ１０１に帰属する移動端末局としての複数のステーション（Station：ＳＴＡ）１０２－１～１０２－ｋとから構成されている。ここに示す無線ＬＡＮシステムは、IEEE802.11で定義するところのインフラストラクチャ方式を採用するものであって、無線ＬＡＮネットワークの最小単位（ＢＢＳ（Basic ServiceSet）４）を構成する。

【０００８】ＢＢＳ４内におけるＡＰ１０１は、各ＳＴＡ１０２－１～１０２－ｋがＡＰ１０１に同期するための情報を含むビーコンフレームを周期的にＢＢＳ４内にブロードキャスト送信する。このビーコンフレームを受信したＢＢＳ４内の各ＳＴＡ１０２－１～１０２－ｋは、通信開始時にＡＰ１０１に対して認証要求を行い、ＡＰ１０１により認証許可を受けた後、ＡＰ１０１との間で通信を行うことが可能となる。なお、図８に示したシステムにおいて、ＡＰ１０１は、「portal」となっているが、この「portal」は、IEEE802.11以外のＬＡＮプロトコルとのプロトコル変換機能をＡＰ１０１に付加していることを意味する。このプロトコル変換機能によりＡＰ１０１と有線ＬＡＮであるイーサネット（登録商標）１０５との接続が可能になっている。

【０００９】上記ＡＰ１０１による認証は、ＭＡＣアドレスによるパケットフィルタ機能を利用した公開鍵認証である。ＡＰ１０１は、認証をしたＳＴＡのＭＡＣアドレスが登録される公開鍵管理テーブルと、自らの秘密鍵であるＡＰ秘密鍵と、これに対応する公開鍵であるＡＰ公開鍵と、これを付したＡＰユーザ証明書とを有する。各ＳＴＡ１０２－１～１０２－ｋは、公開鍵認証を受けたＡＰ１０１のＭＡＣアドレスが登録されるＡＰ情報管理テーブルと、自らの秘密鍵であるＳＴＡ秘密鍵と、これに対応する公開鍵であるＳＴＡ公開鍵と、これを付したＳＴＡユーザ証明書とを有する。

【００１０】各ＳＴＡ１０２－１～１０２－ｋは、以下のような手順でＡＰ１０１による公開鍵認証を受ける。各ＳＴＡ１０２－１～１０２－ｋの公開鍵認証は同じ手順で行われることから、以下の説明では、ＳＴＡ１０２－１を例に挙げて手順を説明する。

【００１１】ＳＴＡ１０２－１は、無線通信を行おうとするＡＰ１０１のＭＡＣアドレスが自身の保持するＡＰ情報管理テーブル内にあるかどうかを確認する。ＡＰ１０１のＭＡＣアドレスがない場合は、ＳＴＡ１０２－１は、ＡＰ１０１に対して公開鍵認証要求を行い、ＡＰ１０１のＭＡＣアドレスがある場合には、ＳＴＡ１０２－１は、ＡＰ１０１に対して公開鍵再認証要求を行う。

【００１２】公開鍵認証要求がなされた場合は、まず、その要求を受信したＡＰ１０１がＳＴＡ１０２－１に対してＡＰユーザ証明書を送信する。次いで、ＳＴＡ１０２－１が、受信したＡＰユーザ証明書を検証した後、そのＡＰユーザ証明書に添付されたＡＰ公開鍵を用いてＳＴＡユーザ証明書を暗号化した暗号化ＳＴＡユーザ証明書をＡＰ１０１へ送信する。次いで、ＡＰ１０１が、受信した暗号化ＳＴＡユーザ証明書をＡＰ秘密鍵で復号化して元のＳＴＡユーザ証明書を再生し、この再生したＳＴＡユーザ証明書を検証した後に、そのＳＴＡユーザ証明書に添付されたＳＴＡ公開鍵を用いて、前回の処理でＳＴＡ１０２－１に対して作成してあった共通鍵を暗号化し、この暗号化共通鍵をＳＴＡ１０２－１へ送信する。最後に、ＳＴＡ１０２－１が、受信した暗号化共通鍵をＳＴＡ公開鍵で復号化して元の共通鍵を再生する。これにより、ＳＴＡ１０２－１は、再生した公開鍵を用いてＡＰ１０１とのフレーム暗号化通信を行うことが可能となる。

【0013】一方、公開鍵再認証要求がなされた場合は、まず、その要求を受信したＡＰ１０１が、ＳＴＡ１０２－１のＭＡＣアドレスおよびＳＴＡ公開鍵の両方が自身の保持する公開鍵管理テーブル内に存在するかどうかを確認し、両方が存在した場合には、ＳＴＡ１０２－１に対して指定する新たな共通鍵を生成し、この生成した新共通鍵をＳＴＡ公開鍵で暗号して暗号化新共通鍵を生成し、この生成した暗号化新共通鍵をＳＴＡ１０２－１に送信して認証許可を通知する。次いで、ＳＴＡ１０２－１が、受信した暗号化新共通鍵をＳＴＡ秘密鍵で復号化して元の新共通鍵を再生する。これにより、ＳＴＡ１０２－１は、再生した新共通鍵を用いてＡＰ１０１とのフレーム暗号化通信を行うことが可能となる。

【0014】

【発明が解決しようとする課題】上述したように、従来の無線ＬＡＮでは、予め定めたシステム管理者が、利用者に対してのみアクセスを許可し、第三者による不正なアクセスを制限するようになっている。しかし、この場合は、システム管理者が固定であるため、システム管理者が会議に参加しない場合は、会議の参加者が、いちいちシステム管理者に対してアクセス許可を得る必要がある、という問題がある。加えて、システム管理者によるアクセス制限は、通常、ＩＤとパスワードにより行われるため、会議の度に、参加者は、システム管理者からＩＤとパスワードを取得する必要があり、アクセスに必要な手続きが煩雑になる、という問題もある。

【0015】図８に示したシステムのように、ＭＡＣアドレスを検査するパケットフィルタ機能を用いることで、よりセキュリティを高めることができる。しかし、このシステムの場合は、各端末（クライアント）に対して公開鍵と秘密鍵とを用いた認証を行う必要があり、やはり処理が煩雑になるという問題がある。

【0016】本発明の目的は、上記各問題を解決し、認証のための処理が煩雑になることがなく、会議の参加者の中からシステム管理者を設定することのできる、無線ＬＡＮシステム、アクセス制御方法およびプログラムを提供することにある。

【0017】

【課題を解決するための手段】上記目的を達成するため、本発明の無線ＬＡＮシステムは、任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線ＬＡＮシステムであって、前記アクセスポイントはサーバを有し、前記サーバは、当該サーバにアクセスしてきた前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって当該サーバへのアクセスが制限される一般ユーザとして扱うように構成されていることを特徴とする。

【0018】本発明のアクセス制御方法は、任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線ＬＡＮシステムにおいて行われるアクセス制御方法であって、前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱い、それ以外の端末の利用者については、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱うことを特徴とする。

【0019】本発明のプログラムは、任意の場所に設置可能なアクセスポイントと、該アクセスポイントと無線により相互通信可能に接続される複数の端末とを有する無線ＬＡＮシステムにおいて用いられるプログラムであって、前記アクセスポイント内に設置されたサーバにアクセスした前記複数の端末のうちの所定の端末の利用者をシステム管理者として扱う処理と、前記所定の端末以外の端末の利用者を、前記システム管理者によって前記サーバへのアクセスが制限される一般ユーザとして扱う処理とを、前記サーバのコンピュータに実行させることを特徴とする。

【0020】上記のとおりの本発明においては、例えば、サーバに最初にアクセスしてきた端末の利用者がシステム管理者とされるので、会議の参加者のだれかがシステム管理者になる。したがって、システム管理者が予め固定された従来のシステムのように、会議の参加者が、いちいちシステム管理者に対してアクセス許可を得る必要はない。

【0021】また、本発明によれば、システム管理者は会議の参加者のうちの一人であり、このシステム管理者により他の端末からのアクセスを制限するようになっている。システム管理者は、通常、会議の参加者に対してのみアクセスが許可することから、第３三者による不正なアクセスは拒否されることになる。また、システム管理者による他の端末からのアクセスの制限にＩＤとパスワードによる認証は必要としないので、従来のようにアクセスに必要な手続きが煩雑になることはない。

【0022】

【発明の実施の形態】次に、本発明の実施形態について図面を参照して説明する。

【0023】図１は、本発明の一実施形態の無線ＬＡＮシステムの概略構成を示すブロック図である。このシステムは、任意の場所に一時的に設置されるアクセスポイント（ＡＰ）１と、このＡＰ１と相互に無線通信可能な複数の端末（クライアント）２－１～２－ｎとを有する。各端末２－１～２－ｎは、所定の無線通信機能（例えば無線ＬＡＮカード）を備える、ノート型ＰＣ端末である。

【0024】ＡＰ１は、Ｗｅｂサーバ１１、ＴＣＰ／ＩＰ（Transmission Control Protocol / Internet Protocol）１２、ＭＡＣドライバ１３、無線ＬＡＮカード１

４およびフィルタテーブル１５を有する。フィルタテーブル１５には、Ｗｅｂサーバ１１への接続要求のあった端末のＭＡＣアドレスが、接続要求を受けた順に登録される。このフィルタテーブル１５へのＭＡＣアドレスの登録はＷｅｂサーバ１１により行われる。ただし、ＡＰ１起動時には、フィルタテーブル１５には何もＭＡＣアドレスは登録されていないものとする。

【００２５】ＴＣＰ／ＩＰ１２、ＭＡＣドライバ１３および無線ＬＡＮカード１４は、プロトコルスタックである。ＴＣＰ／ＩＰ１２は、インターネットワーキングでよく知られた通信プロトコルであって、ＡＰ１と各端末２－１～２－ｎとの間の相互接続を可能とする。このＴＣＰ／ＩＰ１２内部には、ＩＰアドレスとＭＡＣアドレスとの対応をとるためのＡＲＰ（Address Resolution Protocol）テーブル１２１が備えられている。Ｗｅｂサーバ１１は、このＡＲＰテーブル１２１を用いて、各端末２－１～２－ｎから送出されたパケットに含まれる環境変数のＩＰアドレスから接続要求をした端末のＭＡＣアドレスを取得することが可能である。

【００２６】無線ＬＡＮカード１４は、各端末２－１～２－ｎとの無線通信を可能にするためのものである。ＭＡＣドライバ１３は、この無線ＬＡＮカード１４による無線通信を制御するためのデバイスドライバであって、内部にＭＡＣアドレスフィルタ機能１３１を有する。ＭＡＣアドレスフィルタ機能１３１は、上記Ｗｅｂサーバ１１と同様、ＡＲＰテーブル１２１を用いて、各端末２－１～２－ｎから送出されたパケットに含まれる環境変数のＩＰアドレスから接続要求をした端末のＭＡＣアドレスを取得することが可能であり、取得したＭＡＣアドレスと現在のフィルタテーブル１５の内容を参照してパケットの通過許可／禁止を行う。ただし、ＭＡＣアドレスフィルタ機能１３１は、フィルタテーブル１５にＭＡＣアドレスが登録されていない端末からのパケットで、Ｗｅｂサーバ１１宛てのパケットについては無条件に通過させる。

【００２７】Ｗｅｂサーバ１１は、画面生成部１１、管理者判断部１１２およびフィルタテーブル更新部１１３を有する。フィルタテーブル更新部１１３は、Ｗｅｂサーバ１１へアクセス要求した端末のＭＡＣアドレスを、受付順にフィルタテーブル１５に登録する。例えば、最初に受け付けた端末のＭＡＣアドレスは、フィルタテーブル更新部１１３によって順番１の欄に登録される。管理者判断部１１２は、フィルタテーブル１５に最初に登録されたＭＡＣアドレス、すなわち順番１の欄に登録されたＭＡＣアドレスをシステム管理者の端末、それ以外の順番２～Ｎに登録されたＭＡＣアドレスを一般ユーザの端末と判断する。画面生成部１１は、管理者判断部１１２によってシステム管理者と判断された端末に対して、システム管理者である旨の通知を行う。また、画面生成部１１は、システム管理者以外の端末からＷｅｂサーバ１１へ初めてのアクセス要求があった際には、システム管理者の端末に、そのアクセス要求した端末に対するアクセス許可／禁止設定画面を表示して設定作業を促すとともに、その設定結果をフィルタテーブル１５に書き込む。さらに、画面生成部１１は、アクセス要求した端末に対して、システム管理者に対してアクセス許可を要求中である旨の表示、その結果（許可／禁止）の表示などを行う。

【００２８】次に、この無線ＬＡＮシステムの動作について説明する。以下、端末２－１がシステム管理者の端末、それ以外の端末が一般ユーザの端末となるように設定する場合の動作を例にあげて具体的に説明する。

【００２９】ＡＰ１起動直後、まだ、どの端末からもＷｅｂサーバ１１へのアクセス要求が出されていない状態で、端末２－１からＷｅｂサーバ１１に対してアクセス要求を行うと、端末２－１からのパケットは無線ＬＡＮカード１４を通ってＭＡＣドライバ１３に届く。この時点では、フィルタテーブル１５には何も登録されておらず、また、端末２－１から送信されたパケットはＷｅｂサーバ１１宛てのものであるため、その送信パケットはＭＡＣアドレスフィルタ機能１３１による制限を受けることなく、そのままＴＣＰ／ＩＰ１２を通ってＷｅｂサーバ１１に届く。

【００３０】Ｗｅｂサーバ１１では、端末２－１からのパケットを受信すると、まず、受信したパケットの環境変数から取得したＩＰアドレスからＡＲＰテーブル１２１を用いてＭＡＣアドレスを取得する。次いで、フィルタテーブル更新部１１３がフィルタテーブル１５の登録内容を調べる。この時点では、フィルタテーブル１５には何も登録されていないため、フィルタテーブル更新部１１３は、ＭＡＣアドレスをフィルタテーブル１５の順番１の欄に登録する。そして、画面生成部１１１が、端末２－１に対して、システム管理者に設定された旨の通知を行う。このシステム管理者設定通知により、端末２－１の所有者は自分がシステム管理者になってことを確認することができる。

【００３１】上記のシステム管理者設定の後、端末２－１以外の端末、例えば端末２－ｎからＷｅｂサーバ１１に対してアクセス要求を行うと、端末２－ｎからのパケットは無線ＬＡＮカード１４を通ってＭＡＣドライバ１３に届く。この時点では、フィルタテーブル１５の順番１の欄に端末２－１のＭＡＣアドレスが登録されているだけで、端末２－ｎに関するＭＡＣアドレスは登録されておらず、また、端末２－ｎから送信されたパケットはＷｅｂサーバ１１宛てのものであるため、その送信パケットはＭＡＣアドレスフィルタ機能１３１による制限を受けることなく、そのままＴＣＰ／ＩＰ１２を通ってＷｅｂサーバ１１に届く。

【００３２】Ｗｅｂサーバ１１では、端末２－ｎからのパケットを受信すると、まず、受信したパケットの環境

変数から取得したＩＰアドレスからＡＲＰテーブル１２１を用いてＭＡＣアドレスを取得する。次いで、フィルタテーブル更新部１１３が、フィルタテーブル１５の登録内容を調べ、管理者判断部１１２が、その登録内容に基づいて、パケットを送信した端末２－ｎがシステム管理者のものであるかどうかを判断する。具体的には、管理者判断部１１２は、取得した端末２－ｎのＭＡＣアドレスと、フィルタテーブル１５の順番１の欄に登録されたＭＡＣアドレスとが一致するかどうかで、システム管理者の端末かどうかの判断を行う。この時点では、フィルタテーブル１５の順番１の欄には端末２－１のＭＡＣアドレスが登録されているので、管理者判断部１１２は、端末２－ｎからのアクセス要求をシステム管理者以外の端末からのアクセス要求であると判断する。そして、画面生成部１１１が、システム管理者の端末２－１に対して、端末２－ｎからのアクセス許可／禁止設定画面を表示させるとともに、端末２－ｎに対して「管理者に対して許可要求中」の情報表示を行う。

【００３３】端末２－１に表示されたアクセス許可／禁止設定画面上で、システム管理者が、アクセスを許可する、あるいは、アクセスを禁止する旨の設定入力を行うと、画面生成部１１が、その設定入力結果の情報表示を端末２－ｎに対して行うとともに、フィルタテーブル更新部１１３が、フィルタテーブル１５の次に空いている順番２の欄に端末２－ｎのＭＡＣアドレスおよび設定入力結果を登録する。例えば、システム管理者が、アクセスを許可する旨の設定入力を行った場合は、端末２－ｎに「アクセス許可」が表示され、フィルタテーブル１５の順番２の欄には、端末２－ｎのＭＡＣアドレスとともに「アクセス許可」が登録される。反対に、システム管理者が、アクセスを禁止する旨の設定入力を行った場合は、端末２－ｎに「アクセス禁止」が表示され、フィルタテーブル１５の順番２の欄には、端末２－ｎのＭＡＣアドレスとともに「アクセス禁止」が登録される。ここでは、フィルタテーブル１５の順番２の欄に端末２－ｎのＭＡＣアドレスおよび「アクセス許可」の設定入力結果が登録されたものと仮定する。

【００３４】他の端末２－２～２－（ｎ－１）の端末についても、システム管理者設定の後、Ｗｅｂサーバ１１へ初めてアクセス要求を行った場合には、上記の端末２－ｎと同様の手順で、それぞれのＭＡＣアドレスおよびシステム管理者によるアクセス許可／禁止の設定結果がフィルタテーブル１５に登録される。

【００３５】次に、各端末２－１～２－ｎからのＷｅｂサーバ１１への２回目以降のアクセスの際の動作について説明する。

【００３６】端末２－１からＷｅｂサーバ１１へ２回目のアクセス要求を行うと、端末２－１からのパケットは無線ＬＡＮカード１４を通ってＭＡＣドライバ１３に届く。この時点では、フィルタテーブル１５の順番１の欄に端末２－１のＭＡＣアドレスが登録されており、しかも、この順番１はシステム管理者であることを示すものであるため、ＭＡＣアドレスフィルタ機能１３１は、その送信パケットをそのままＴＣＰ／ＩＰ１２を介してＷｅｂサーバ１１に送出する。

【００３７】Ｗｅｂサーバ１１では、パケットを受信すると、まず、受信したパケットの環境変数から取得したＩＰアドレスからＡＲＰテーブル１２１を用いてＭＡＣアドレスを取得する。次いで、フィルタテーブル更新部１１３が、フィルタテーブル１５の登録内容を調べ、管理者判断部１１２が、その登録内容に基づいて、パケットを送信した端末２－１がシステム管理者のものであるかどうかを判断する。この時点では、フィルタテーブル１５の順番１の欄には、端末２－１のＭＡＣアドレスが登録されているので、管理者判断部１１２は、パケットを送信した端末２－１をシステム管理者の端末として取り扱う。これにより、Ｗｅｂサーバ１１と端末２－１との間で必要なデータの授受が可能になる。

【００３８】一方、端末２－１以外の端末、例えば端末２－ｎからＷｅｂサーバ１１へ２回目のアクセス要求を行うと、端末２－ｎからのパケットは無線ＬＡＮカード１４を通ってＭＡＣドライバ１３に届く。この時点では、フィルタテーブル１５の順番２の欄に端末２－ｎのＭＡＣアドレスが登録されており、しかも、この順番２の欄には「アクセス許可」の設定入力結果が登録されているので、ＭＡＣアドレスフィルタ機能１３１は、その送信パケットをそのままＴＣＰ／ＩＰ１２を介してＷｅｂサーバ１１へ送出する。なお、順番２の欄に登録されている設定入力結果が「アクセス禁止」である場合は、ＭＡＣアドレスフィルタ機能１３１は、端末２－ｎからのパケットを廃棄する。

【００３９】Ｗｅｂサーバ１１では、パケットを受信すると、まず、受信したパケットの環境変数から取得したＩＰアドレスからＡＲＰテーブル１２１を用いてＭＡＣアドレスを取得する。次いで、フィルタテーブル更新部１１３が、フィルタテーブル１５の登録内容を調べ、管理者判断部１１２が、その登録内容に基づいて、パケットを送信した端末２－１がシステム管理者のものであるかどうかを判断する。端末２－ｎのＭＡＣアドレスは、フィルタテーブル１５の順番２の欄に登録されているため、管理者判断部１１２は、パケットを送信した端末２－ｎを、システム管理者によってアクセス許可が許された一般ユーザの端末として取り扱う。これにより、Ｗｅｂサーバ１１と端末２－ｎとの間で必要なデータの授受が可能になる。

【００４０】以上のように、本実施形態の無線ＬＡＮシステムによれば、Ｗｅｂサーバ１１は、最初にアクセスしてきた端末をシステム管理者の端末とするようになっているので、会議の参加者のだれかがシステム管理者になることになる。

【００４１】また、フィルタテーブル１５に登録されていない端末は、Ｗｅｂサーバ１１へアクセスを要求する際には、必ず、設定されたシステム管理者によってアクセスの許可／禁止の設定がなされるため、システム管理者が会議の参加者に対してのみアクセスを許可するようにすれば、第３者による不正なアクセスを防止することができる。

【００４２】

【実施例】図２は、本発明の無線ＬＡＮシステムの一実施例を示すブロック図である。本実施例のシステムは、図１に示したシステムを、「Ｗｉｎｄｏｗｓ」（マイクロソフト社製）を搭載したＰＣ上で作成した「Ｗｉｎｄｏｗｓ」共有ファイルに対するアクセス制限を行うシステムに適用したもので、その構成は「Ｗｉｎｄｏｗｓ」共有ファイル２０、Ｗｅｂサーバ２１、ＴＰＣ／ＩＰ２２、ＭＡＣドライバ２３、無線ＬＡＮカード２４およびフィルタテーブル２５からなるアクセスポイントと、これに無線により相互通信可能に接続される２台の端末２ａ、２ｂとから構成されている。Ｗｅｂサーバ２１、ＴＰＣ／ＩＰ２２、ＭＡＣドライバ２３、無線ＬＡＮカード２４およびフィルタテーブル２５は、図１に示したシステムのものと基本的に同じものである。

【００４３】「Ｗｉｎｄｏｗｓ」共有ファイル２０は、例えばＵＮＩＸ（登録商標）では、ＳＡＭＢＡと呼ばれるアプリケーションで実現することができる。また、Ｗｅｂサーバ２１は、ＵＮＩＸでは、「Ａｐａｃｈｅ」というアプリケーションで実現することができる。Ｗｅｂサーバ２１は、アクセスを要求した端末に対してＷｅｂ画面の表示を行うとともに、前述の実施形態で説明したようにフィルタテーブル２５へ必要なデータの登録および参照を行う。

【００４４】２台の端末２ａ、２ｂは無線ＬＡＮ端末で、それぞれＩＰアドレスおよびＭＡＣアドレスを以下のように設定している。

【００４５】

端末２ａ：ＩＰ＝192.168.1.1　ＭＡＣ＝000042-8A9C01

端末２ｂ：ＩＰ＝192.168.1.2　ＭＡＣ＝000042-8A9C02

ここで、ＭＡＣアドレス中の「-」は、アドレス表記を見易いものにするために挿入したものである。

【００４６】次に、本実施例のシステムの動作を具体的に説明する。図３は、図２のシステムにおけるＭＡＣドライバ２３のＭＡＣアドレスフィルタ機能におけるフィルタ処理手順を示すフローチャートである。図４は、図２のシステムにおけるＷｅｂサーバ２１の動作を示すフローチャートである。

【００４７】まず、端末２ａがＷｅｂサーバ２１にアクセスしたときの動作について説明する。

【００４８】端末２ａがＷｅｂサーバ２１にパケットを送信すると、この送信パケットは、無線ＬＡＮカード２４を経由してＭＡＣドライバ２３に届く。このＭＡＣドライバ２３では、ＭＡＣアドレスフィルタ機能により、図３に示す以下のような手順でフィルタ処理が行われる。

【００４９】ステップＳ１０で、端末２ａのＭＡＣアドレスがフィルタテーブル２５に登録されているかどうかが判断される。この端末２ａからＷｅｂサーバ２１へのアクセスは初めてのアクセスであるため、この時点では、端末２ａのＭＡＣアドレスはフィルタテーブル２５に登録されていない。したがって、このステップＳ１０での判断における分岐は「Ｎ」となり、続くステップＳ１２に移行する。なお、端末２ａのＭＡＣアドレスがフィルタテーブル２５に登録されている場合は、分岐は「Ｙ」となり、ステップＳ１１でパケットを通すことになる。

【００５０】ステップＳ１２では、端末２ａのアクセスがＷｅｂサーバへのアクセスかどうかの判断が行われる。この端末２ａからのアクセスはＷｅｂサーバへのアクセスであるので、このステップＳ１１での判断における分岐は「Ｙ」となり、続くステップＳ１３でパケットを通すことになる。なお、Ｗｅｂサーバへのアクセスでない場合は、分岐は「Ｎ」となり、続くステップＳ１４でパケットは破棄される。

【００５１】上記のようにして、端末２ａからのパケットはＭＡＣアドレスフィルタ機能によるフィルタ処理を受けた後、ＴＣＰ／ＩＰ２２を通ってＷｅｂサーバ２１に届く。

【００５２】次に、端末２ａからのパケットを受信したＷｅｂサーバ２１の動作を、図４を参照して説明する。

【００５３】ステップＳ２０で、端末２ａからのパケットの環境変数から端末２ａのＩＰアドレス「192.168.1.1」を取得する。続くステップＳ２１で、ＴＣＰ／ＩＰ２２内部のＡＲＰテーブルを用いてその取得したＩＰアドレスから端末２ａのＭＡＣアドレス「000042-8A9C01」を取得する。次いで、ステップＳ２２で、その取得したＭＡＣアドレスがフィルタテーブル２５に登録されているかどうかを調べる。この時点では、端末２ａからのアクセスは初めてのアクセスであるので、フィルタテーブル２５には端末２ａのＭＡＣアドレスは登録されていない。したがって、ステップＳ２２における分岐は「Ｎ」となり、続くステップＳ２６でフィルタテーブル２５への登録を行う。ここでは、端末２ａを当該Ｗｅｂサーバへ最初にアクセスした端末と仮定し、端末２ａのＭＡＣアドレスをフィルタテーブル２５の１番の欄に登録する。

【００５４】ステップＳ２６にて端末２ａのＭＡＣアドレスのフィルタテーブル２５への登録がなされると、続いて、ステップＳ２７で、フィルタテーブル２５への登録が１番の欄への登録であったどうかが判断される。ステップＳ２６で、端末２ａのＭＡＣアドレスをフィルタテーブル２５の１番の欄に登録したので、ステップＳ２

7における分岐は「Y」となり、続くステップS28で端末2aに対して管理者用画面表示を行う。これにより、端末2aの利用者は、システム管理者として他の端末のアクセスの許可／禁止を制限することが可能となる。

【0055】次に、端末2bがWebサーバ21へアクセスした場合の動作について説明する。

【0056】端末2bがWebサーバ21にパケットを送信すると、この送信パケットも、上述の端末2aの場合と同様に、無線LANカード24を経由してMACドライバ23に届く。MACドライバ23では、MACアドレスフィルタ機能により以下のような手順でフィルタ処理が行われる（図3参照）。

【0057】ステップS10で、端末2bのMACアドレスがフィルタテーブル25に登録されているかどうかが判断される。この端末2bからWebサーバ21へのアクセスは初めてのアクセスであるため、この時点では、端末2bのMACアドレスはフィルタテーブル25に登録されていない。したがって、このステップS10での判断における分岐は「N」となり、続くステップS12に移行する。

【0058】ステップS12では、端末2aのアクセスがWebサーバ21へのアクセスかどうかの判断が行われる。この端末2aからのアクセスはWebサーバ21へのアクセスであるので、このステップS11での判断における分岐は「Y」となり、続くステップS13でパケットを通すことになる。

【0059】上記のようにして、端末2bからのパケットはMACアドレスフィルタ機能によるフィルタ処理を受けた後、TCP／IP22を通ってWebサーバ21に届く。

【0060】次に、端末2bからのパケットを受信したWebサーバ21の動作を説明する（図4参照）。

【0061】ステップS20で、端末2bからのパケットの環境変数から端末2bのIPアドレス「192.168.1.2」を取得する。続くステップS21で、TCP／IP22内部のARPテーブルを用いてその取得したIPアドレスから端末2bのMACアドレス「000042-8A9C02」を取得する。次いで、ステップS22で、その取得したMACアドレスがフィルタテーブル25に登録されているかどうかを調べる。この時点では、端末2bからのアクセスは初めてのアクセスであるので、フィルタテーブル25には端末2bのMACアドレスは登録されていない。したがって、ステップS22における分岐は「N」となり、続くステップS26でフィルタテーブル25への登録を行う。フィルタテーブル25の1番の欄には端末2aのMACアドレスがすでに登録されているので、端末2bのMACアドレスは2番の欄に登録される。

【0062】ステップS26にて端末2bのMACアドレスのフィルタテーブル25への登録がなされると、続いて、ステップS27で、フィルタテーブル25への登録が1番の欄への登録であったどうかが判断される。ステップS26で、端末2bのMACアドレスをフィルタテーブル25の2番の欄に登録したので、ステップS27における分岐は「N」となり、続くステップS29で端末2aに対して端末2bに関するアクセス要求画面表示を行う。これにより、端末2aの利用者であるシステム管理者は、表示されたアクセス要求画面上で端末2bに対してアクセスの許可／禁止を制限することができる。

【0063】上記ステップS29で、システム管理者が端末2bに対してアクセスの禁止を設定した場合は、Webサーバ21は、上記ステップS26で順番2の欄に登録した端末2bのMACアドレスを削除する。システム管理者が端末2bに対してアクセスの許可を設定した場合は、上記ステップS26で順番2の欄に登録した端末2bのMACアドレスはそのまま保持される。上記ステップS29で、システム管理者が端末2bに対してアクセスの許可を設定した場合の、フィルタテーブル25の登録内容の一例を図5に示す。図5の例では、順番「1」の欄に端末2aのMACアドレス「000042-8A9C01」が登録され、さらに順番「2」の欄に端末2bのMACアドレス「000042-8A9C02」が登録されている。このフィルタテーブル25は、MACアドレスフィルタ機能におけるフィルタ処理の際に用いられ、以降端末2bからのすべてのパケットがこのMACアドレスフィルタ機能を通過することとなる。

【0064】次に、端末2a、2bからの2回目以降のアクセスについて簡単に説明する。

【0065】端末2aからの2回目以降のアクセスの場合は、図3のステップS10の分岐で「Y」となり、端末2aからのパケットがWebサーバ21に届く。Webサーバ21では、図4のステップS22の分岐で「Y」となり、続くステップS23で1番の欄に登録されているか否かの判断がなされる。端末2aのMACアドレスはフィルタテーブル25の1番の欄に登録されているので、この判断における分岐は「Y」となり、続くステップS24で、端末2aに対して再び管理者用画面表示が行われる。

【0066】端末2bからの2回目以降のアクセスの場合は、図3のステップS10の分岐で「Y」となり、端末2bからのパケットがWebサーバ21に届く。Webサーバ21では、図4のステップS22の分岐で「Y」となり、続くステップS23で1番の欄に登録されているか否かの判断がなされる。端末2bのMACアドレスはフィルタテーブル25の2番の欄に登録されているので、この判断における分岐は「Y」となり、続くステップS24で、端末2bに対して一般者用画面表示が行われる。ここで、一般者用画面表示は、例えば、会

議に関する情報一覧である。端末２ｂの利用者は、その情報一覧から所望の項目、例えばＷｉｎｄｏｗｓ共有ファイル２０を選択することで必要な情報を入手することができる。

【００６７】なお、システム管理者からアクセス許可を得る前に端末２ｂからＷｉｎｄｏｗｓ共有ファイル２０へ直接アクセスが行われた場合は、図３のステップＳ１０の分岐が「Ｎ」となり、続くステップＳ１２の分岐が「Ｎ」となって、ステップＳ１４で端末２ｂからのパケットが廃棄される。

【００６８】上述した本実施例の無線ＬＡＮシステムの構成および動作は一例であり、種々変更が可能である。例えば、図４のステップＳ２９で、端末２ａの利用者であるシステム管理者が、表示されたアクセス要求画面上で端末２ｂに対してアクセスの許可／禁止を制限する設定入力を行った場合に、その設定入力結果をフィルタテーブル２５に登録するようにしてもよい。その場合のフィルタテーブル２５の一例を図６に示す。図６の例では、順番「１」の欄に端末２ａのＭＡＣアドレス「000042-8A9C01」が登録され、さらに順番「２」の欄に端末２ｂのＭＡＣアドレス「000042-8A9C02」および設定入力結果「アクセス許可」が登録されている。この場合は、ＭＡＣアドレスフィルタ機能は、フィルタテーブル２５に登録された設定入力結果を参照してフィルタ処理を行うことになる。

【００６９】以上説明した実施形態および実施例では、ＡＰ起動後、Ｗｅｂサーバに対して最初にアクセスした端末をシステム管理者として設定するようになっているが、本発明はこれに限定されるものではなく、会議の参加者のだれかにシステム管理者を設定することができるのであれば、どのような構成としてもよい。例えば、Ｗｅｂサーバへのアクセス時に、「自分をシステム管理者として登録する」というチェックボックスを設けたアクセス画面が端末に表示されるようにし、このチェックボックスをチェックした形でアクセス要求を行った端末に対してシステム管理者の設定を行うようにしてもよい。

【００７０】また、ＡＰは、他の有線ＬＡＮと接続されていてもよい。ＡＰが他の有線ＬＡＮと接続されたシステムとしては、例えば図８に示した従来のシステムに本発明の無線ＬＡＮシステムの構成を適用したものが考えられる。

【００７１】また、アクセスポイント内に設けられるサーバやＭＡＣアドレスフィルタ機能、および端末などは、周知のコンピュータシステムによって実現することができる。図７は、そのようなコンピュータシステムの一形態を示すブロック図である。このコンピュータシステムは、プログラムなどを蓄積する記憶装置３１、キーボードやマウスなどの入力装置３２、ＣＲＴやＬＣＤなどの表示装置３３、外部との通信を行うモデムなどの通信装置３４、プリンタなどの出力装置３５および入力装置からの入力を受け付けて通信装置、出力装置、表示装置の動作を制御する制御装置（ＣＰＵ）３０から構成されている。例えば、図２のシステムのサーバをこのコンピュータシステムを用いて構成する場合は、記憶装置３１に図４に示した処理手順を実行するためのプログラムが予め記憶され、制御装置３０がそのプログラムを読出して実行することになる。なお、プログラムは、不図示の記録媒体（ＣＤ－ＲＯＭ）などで提供されてもよい。

【００７２】

【発明の効果】以上説明したように、本発明によれば、システム管理者は会議の参加者の中から設定される。したがって、従来のように会議に参加しないシステム管理者に対していちいちアクセス許可を得る必要がなく、より利用し易いシステムを提供することができる。

【００７３】また、本発明によれば、システム管理者は、会議の参加者が利用者となっている端末に対してのみアクセスを許可するので、第３者による不正なアクセスを確実に防止することができる。

【００７４】さらに、本発明によれば、システム管理者によるアクセス制限に、ＩＤとパスワードによる認証を必要としないので、処理手順の簡単化、処理時間の短縮を図ることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態の無線ＬＡＮシステムの概略構成を示すブロック図である。

【図２】本発明の無線ＬＡＮシステムの一実施例を示すブロック図である。

【図３】図２に示すシステムにおけるＭＡＣアドレスフィルタ機能によるフィルタ処理手順を示すフローチャート図である。

【図４】図２に示すシステムにおけるＷｅｂサーバの動作を示すフローチャート図である。

【図５】図２に示すシステムで用いられるフィルタテーブルの登録内容の一例を示す図である。

【図６】図２に示すシステムで用いられるフィルタテーブルの登録内容の他の例を示す図である。

【図７】本発明の無線ＬＡＮシステムに適用可能なコンピュータシステムの一形態を示すブロック図である。

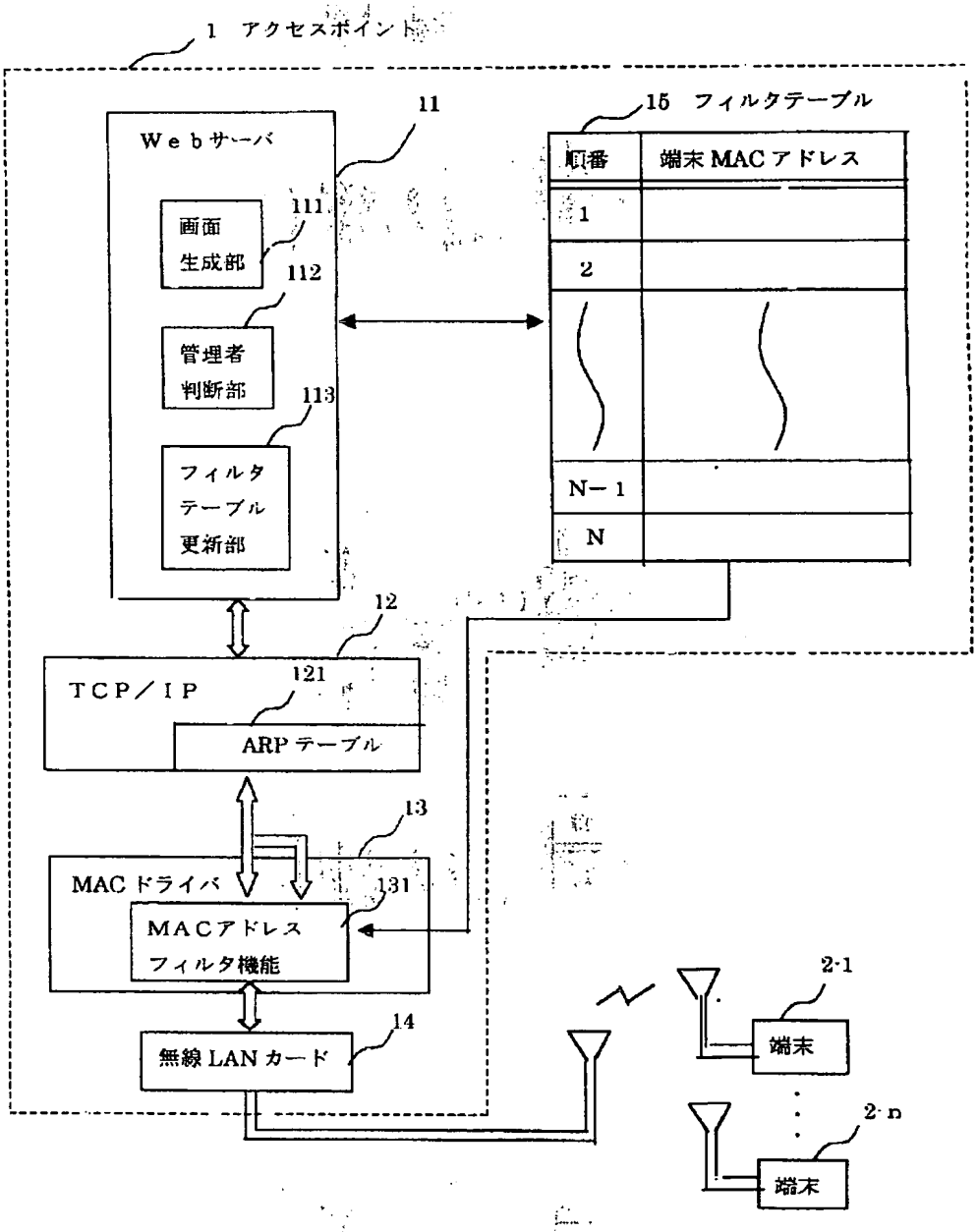
【図８】従来の無線ＬＡＮシステムの概略構成を示すブロック図である。

【符号の説明】

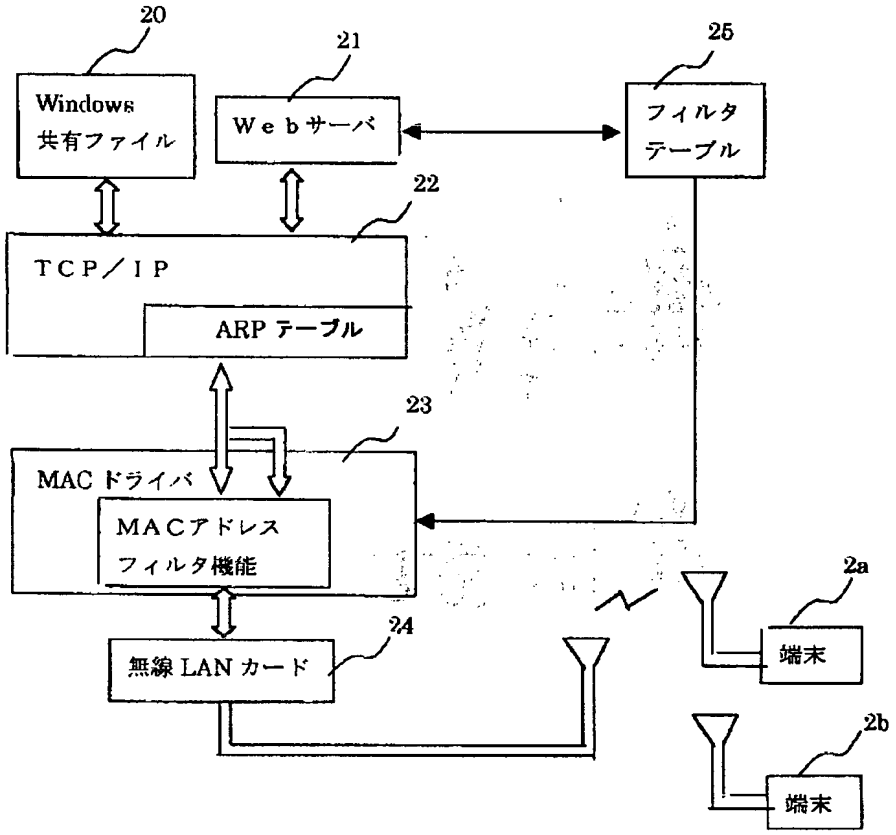
１、１０１　アクセスポイント
２－１～２－ｎ、２ａ、２ｂ　端末
１１、２１　Ｗｅｂサーバ
１２、２２　ＴＣＰ／ＩＰ
１３、２３　ＭＡＣドライバ
１４、２４　無線ＬＡＮカード
１５、２５　フィルタテーブル
２０　Ｗｉｎｄｏｗｓ共有ファイル
３０　制御装置

31　記憶装置
32　入力装置
33　表示装置
34　通信装置
35　出力装置
102-1～102-k　STA
104　BBS
105　イーサネット
111　画面生成部
112　管理者判断部
113　フィルタテーブル更新部
121　ARPテーブル
131　MACアドレスフィルタ機能

【図1】



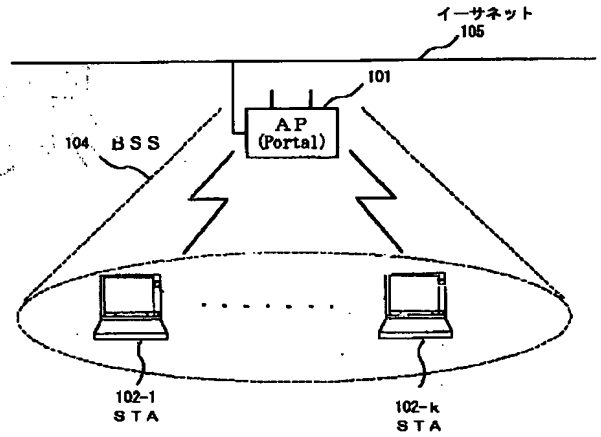
【図2】



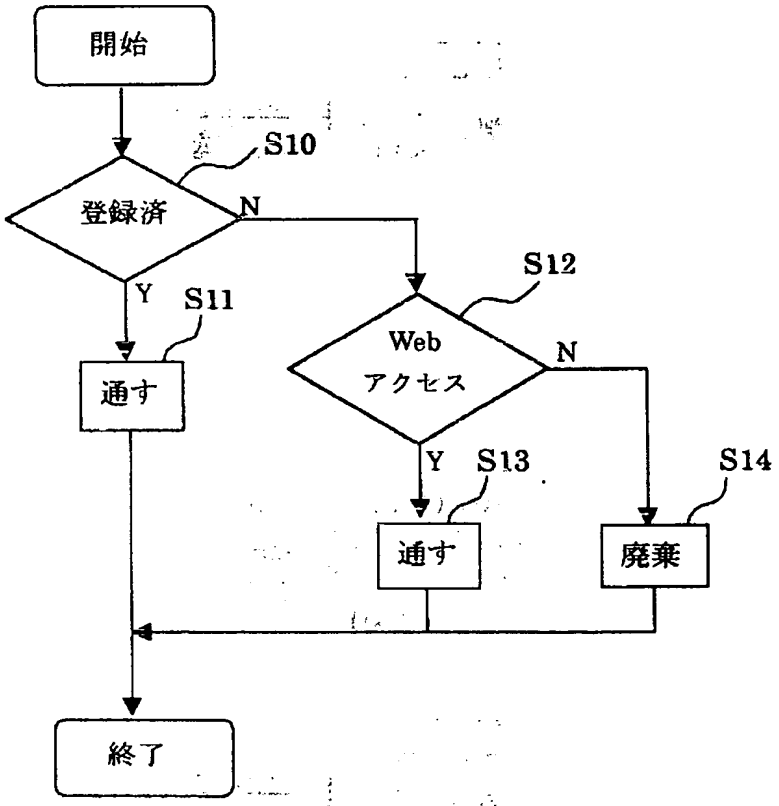
【図5】

順番	MACアドレス
1	000042·8A9C01
2	000042·8A9C02
≀	≀

【図8】



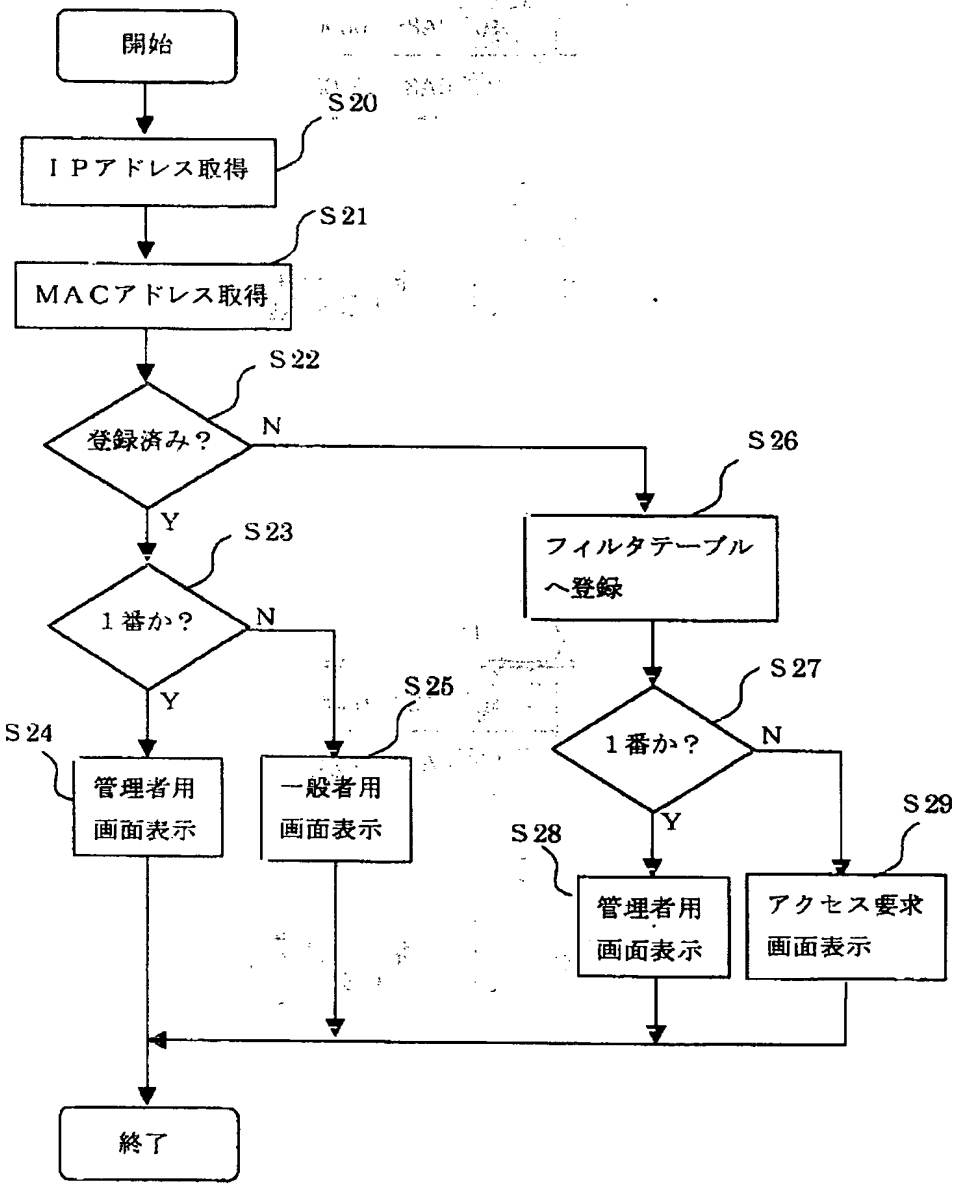
【図3】



【図6】

順番	MACアドレス	設定入力結果
1	000042-8A9C01	
2	000042-8A9C02	アクセス許可
～	～	～

【図４】


開始
S20
ＩＰアドレス取得
S21
ＭＡＣアドレス取得
S22
登録済み？
N
Y
S23
１番か？
N
Y
S24
管理者用
画面表示
S25
一般者用
画面表示
S26
フィルタテーブル
へ登録
S27
１番か？
N
Y
S28
管理者用
画面表示
S29
アクセス要求
画面表示
終了

【図7】